UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF SECOND FLOOR, SUITE #2, 919 LAFAYETTE ROAD, SEABROOK, NEW HAMPSHIRE 03874 and SECOND FLOOR, SUITE #8, 919 LAFAYETTE ROAD, SEABROOK ,NEW HAMPSHIRE 03874	Case No. 19-mj- 232-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANTS

I, Special Agent Ron Morin, being duly sworn, depose and state the following:

1. I am a Special Agent with the U.S. Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), and have been so employed since May 2006. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as a Special Agent, I investigate criminal violations relating to a broad range of immigration and customs-related statutes and have been cross designated to investigate violations relating to the distribution of illicit narcotics as specified under Title 21 of the U.S. Code. I have been trained in drug investigations, narcotics identification, search warrants, undercover techniques, surveillance, debriefing of informants, and other investigative procedures. Through my training, education, and experience, I have become familiar generally with the manner in which drug distribution organizations conduct their illegal activities, including purchasing, manufacturing, storing, and distributing narcotics, the laundering of illegal proceeds, and the efforts of persons involved in such activity to avoid detection by law enforcement. In the course of participating in investigations of drug distribution organizations, I have conducted or participated in surveillance, the purchase of illegal drugs, the execution of

search warrants, the use of tracking devices, debriefings of subjects, witnesses, and informants, and reviews of consensually recorded conversations and meetings.

2. The information contained in this affidavit is based on my personal participation in the investigation of this case and information provided to me by other federal, state, and local law enforcement agents and officers, and other information and data gathered during the course of this investigation. All observations that were not made personally by me were related to me by the persons who made the observations. This affidavit is not intended to include each and every fact and matter observed by me or known to the government relating to the subject matter of this investigation. Instead, this affidavit contains only those facts which are necessary to establish that probable cause exists to prove that fruits, evidence, and instrumentalities of the offenses described herein will be found at the locations to be searched.

3. On November 12, 2019, this Court granted search warrants for, inter alia, two businesses located at 919 Lafayette Road, Seabrook, New Hampshire, called Leather and Lace and Up N Smoke. Those warrants were based on probable cause that the owner of those businesses, William F. Walsh ("WALSH"), and others, both known and unknown have committed violations of 21 U.S.C. § 841 (Distribution of Controlled Substances) and 21 U.S.C. § 846 (Conspiracy to Distribute Controlled Substances). The affidavit in support of the search warrants for Leather and Lace and Up N Smoke (among other locations), is attached hereto as Attachment A and is incorporated by reference.

4. On November 14, 2019, officers and agents for the Department of Homeland Security, United States Drug Enforcement Administration, United States Postal Service, and the Seabrook, New Hampshire Police Department executed the search warrants for Leather and Lace and Up N Smoke at 919 Lafayette Road, Seabrook, New Hampshire, referred to above. When the

officers and agents did so, they learned that there is a second front door to the building located at 919 Lafayette Road that leads upstairs to a second floor where there are a series of office suites.

5. On the morning of November 14, 2019, Detective Michael Maloney interviewed Tommy Cook. Cook is the store manager for Leather and Lace and Up N Smoke. Cook indicated that he had worked for WALSH for approximately 18 years. Cook stated that he and WALSH used two of the second floor office suites, suites #2 and #8, for work related to Leather and Lace and Up N Smoke. He also said that materials related to those businesses were stored in those suites. Cook stated that as recently as November 13, 2019, he had been working in suite #8 on matters related to Up N Smoke and/or Leather and Lace.

6. On the same morning, Cook escorted Detective Maloney to the second floor of 919 Lafayette Road and pointed out suite #2 and suite #8 as the offices that he used for business related to Up N Smoke and Leather and Lace. The suites are located across the hall from one another. Above the door of each suite is a sign providing the identifying suite number. The wood doors to the suites are adjacent to glass panes. Through the panes, Detective Maloney saw in both suites paperwork of various sorts. In suite #2, he saw a fax machine and mail addressed to Up N Smoke.

7. Law enforcement asked WALSH if he would consent to the search of suites #2 and #8. He refused those requests.

8. Based on the information discussed above, the specific items to be seized are described and detailed in Attachment C.

9. Based on the information provided in this affidavit and in Attachment A, I submit that there is probable cause to believe that the items set forth in Attachment C will be found within suites #2 and #8 and that such items constitute evidence related to the distribution of

controlled substances, and any attempts and/or conspiracies to do the same, in violation of Title 21, United States Code, Sections 841(a)(1) and 846.

10. Wherefore, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, I respectfully request warrants to search 919 Lafayette Road, suites #2 and #8, Seabrook, New Hampshire, which are all located within the District of New Hampshire.

11. I declare under penalty of perjury that the statements above are true and correct to the best of my knowledge and belief.

/s/ Ron Morin
Ron Morin
Special Agent
Homeland Security Investigations

Sworn and subscribed to me on 11/14, 2019.

The Honorable Andrea K. Johnston
United States Magistrate Judge

ATTACHMENT B

PREMISES TO BE SEARCHED

The properties to be searched are the following:

- **Suite #2, 919 Lafayette Road, Second Floor, Seabrook, New Hampshire.** is an individual second floor room with a wooden door and adjacent glass panes. Above the door to the suite is a sign stating suite #2.
- **Suite #8, 919 Lafayette Road, Second Floor, Seabrook, New Hampshire.** is an individual second floor room with a wooden door and adjacent glass panes. Above the door to the suite is a sign stating suite #8.

ATTACHMENT C

LIST OF ITEMS AUTHORIZED TO BE SEARCHED-FOR AND SEIZED PURSUANT TO FEDERAL SEARCH WARRANT

The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841 and 846, pertaining to the distribution of controlled substances (the Subject Offenses), namely:

a. Controlled substances and/or controlled substances residue, indicia of distribution (such as scales or packaging materials), records and documents, receipts, notes ledgers, and other papers including any computerized or electronic records, including cellular telephones, relating to the ordering, purchase, or possession of controlled substances;

b. Records and documents, receipts, notes ledgers and other papers including any computerized or electronic records including cellular telephones, relating to the laundering of money or structuring of financial transactions;

c. United States currency, financial instruments — including but not limited to stocks and bonds — and other illicit gains;

d. Address and/or telephone books, appointment logs, daily or monthly planners, Rolodexes, meeting schedules, any and all materials reflecting names, addresses, telephone numbers, pager numbers, fax numbers and/or telex numbers of co-conspirators, including any individuals with whom a financial relationship exists, as well as financial institutions and other individuals or businesses with whom a financial relationship exists;

e. Photographs, including still photos, negatives, video tapes, films, undeveloped film and the contents therein, in particular photographs of co-conspirators, of assets and/ or controlled substances;

f. Indicia of occupancy, residency, rental and/ or ownership of the premises described herein, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchases or lease agreements, and keys;

g. Tickets, notes, receipts, and other items relating to domestic and international travel, including but not limited to, airline tickets, boarding passes, airline receipts, car rental agreements, commercial bus tickets, passports, and visas;

h. Any locked or closed containers including but not limited to safes, both combination and lock type, and their contents, which could include any of the above listed evidence;

i. Books and records of corporations, partnerships, trusts and/or businesses, both domestic and foreign, including but not limited to: articles of incorporation or other formation or dissolution documents, bylaws, minutes of any corporate, board or shareholder's meeting, stock registers or other records identifying corporate shareholders, records reflecting the true or beneficial owner of any business, documentation evidencing the secreting, movement, transfer, or conversion of assets, both monetary and non-monetary, records identifying shareholders, partners, directors, or officers, personnel or payroll records, income or excise tax returns and/or copies, corporate seals, financial statements, journals, ledgers, notes, workpapers, real estate transaction records, bank statements and related records, brokerage account statements and related records, cancelled checks, deposit slips and other items, withdrawal slips and other items, passbooks, letters of credit, credit card statements and receipts, money orders, bank drafts and cashiers checks, bank checks, safe deposit box keys, receipts, invoices, lease agreements, correspondence, agreements, declarations, certifications, powers-of-attorney and other items evidencing the ownership or control of other business entities, and other items evidencing income, expenditures, assets, liabilities or investments;

j. Books and records of personal income, expenditures or investments, both domestic and foreign, including but not limited to: income or excise tax returns and/or copies, financial statements, journals, ledgers, notes, workpapers, bank statements and related records, cancelled checks, passbooks, letters of credit, credit card statements and receipts, money orders, bank drafts and cashiers checks, bank checks, safe deposit box keys, brokerage or other financial institution transaction statements, stocks, bonds, mortgages, real estate transaction records, receipts, invoices, and other items evidencing income, expenditures, assets, liabilities or investments;

k. Records of loans, contracts, mortgages, notes, agreements, applications, schedules, records of payments, financing statements, collateral records, and other financial records;

l. Records relating to the use of landline, credit card, and cellular telephone services, including cellular telephones, facsimile machines and the stored electronic communications therein, as well as documentation containing telephone, credit card, and computer access codes;

m. Records relating to the rental of post office boxes or drop boxes, domestic and foreign;

n. All documents reflecting the names of personal aliases, corporate entities, shell corporations, partnerships, relatives and associates (nominees);

o. Logs of electronic communications, disks of communications, hard copies of communications, audio cassette tapes of communications, calendars, appointment books, telephone number lists, incoming and outgoing facsimile messages, and any documentation, telephone records, bank account information or wire transfer information;

p. Electronic equipment, including but not limited to computers, facsimile machines, currency counting machines, telephone answering machines used to generate, transfer, count, record, and/or store the information described in the above-listed evidence. Additionally, computer software, tapes, discs, audio tapes, flash drives, memory sticks, PDAs, cellular telephones, and the contents therein, containing the information generated by the aforementioned electronic equipment.

As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICES

In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

During the execution of this search warrant, law enforcement is permitted to: (1) depress WALSH's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of WALSH's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

NOTE: Any wireless or cellular telephones shall be searched for the information set forth in this Attachment including recent calls, contact lists, stored text messages, emails, and any other stored files or data.

The search authorized by this Warrant for the subject property is of the entire premises, including all buildings, outbuildings, garages, yard areas, trash containers, storage areas, vehicles and containers used in connection with or within the curtilage of the Target Locations.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE RESIDENCE AND BUSINESSES LOCATED AT: 35 JEAN DRIVE, SEABROOK, NEW HAMPSHIRE 03874 **(Target Location 1)** SMOKING MONKEY INC., 14 LOWER NEW ZEALAND ROAD SEABROOK, NEW HAMPSHIRE 03874 **(Target Location 2)** UP N SMOKE, 919 LAFAYETTE ROAD SEABROOK, NEW HAMPSHIRE 03874 **(Target Location 3)** LEATHER & LACE ADULT VIDEOS, 919 LAFAYETTE ROAD SEABROOK, NEW HAMPSHIRE 03874 **(Target Location 4)**	Case No. 19-sw- _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEARCH WARRANTS

I, Special Agent Derek Dunn, being duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), and have been so employed since April 2003. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as a Special Agent, I investigate criminal violations relating to a broad range of immigration and customs-related statutes and have been cross designated to investigate violations relating to the distribution of illicit narcotics as specified under Title 21 of

ATTACHMENT A

the U.S. Code. I have been trained in drug investigations, narcotics identification, search warrants, undercover techniques, surveillance, debriefing of informants, and other investigative procedures. Through my training, education, and experience, I have become familiar generally with the manner in which drug distribution organizations conduct their illegal activities, including purchasing, manufacturing, storing, and distributing narcotics, the laundering of illegal proceeds, and the efforts of persons involved in such activity to avoid detection by law enforcement. In the course of participating in investigations of drug distribution organizations, I have conducted or participated in surveillance, the purchase of illegal drugs, the execution of search warrants, the use of tracking devices, debriefings of subjects, witnesses, and informants, and reviews of consensually recorded conversations and meetings.

2. The information contained in this affidavit is based on my personal participation in the investigation of this case and information provided to me by other federal, state, and local law enforcement agents and officers, and other information and data gathered during the course of this investigation. All observations that were not made personally by me were related to me by the persons who made the observations. This affidavit is not intended to include each and every fact and matter observed by me or known to the government relating to the subject matter of this investigation. Instead, this affidavit contains only those facts which are necessary to establish that probable cause exists to prove that fruits, evidence, and instrumentalities of the offenses described herein will be found at the locations to be searched.

3. Based on my training, experience, and the facts as set forth in this affidavit, I submit that there is probable cause to believe that William F. Walsh ("WALSH"), and others, both known and unknown have committed violations of 21 U.S.C. § 841 (Distribution of Controlled Substances) and 21 U.S.C. § 846 (Conspiracy to Distribute Controlled Substances).

TARGET LOCATIONS

4. I make this affidavit in support of three applications for search warrants under Rule 41 of the Federal Rules of Criminal Procedure for three locations, collectively the "**Target Locations**," and any and all structures and/or vehicles within the curtilage thereof, all of which are located within Rockingham County, within the District of New Hampshire. The **Target Locations** to be searched are described in further detail in Attachment A and the things to be searched for within the **Target Locations** are described in further detail in Attachment B.

5. WALSH has been identified as the owner, operator, and President of Smoking Monkey, Inc. In business filings, WALSH is listed as the Principal of Smoking Monkey, Inc which has a listed line of business of "Whol [sic] Farm Product Raw Materials." The business name, Smoking Monkey Inc sometimes noted as Smoker's City LTD and S.M.I., is known to currently operate retail establishments under the names the Smoking Monkey, which is physically located at 14 New Zealand Road, Seabrook, New Hampshire 03874 (**Target Location 2**) and Up N Smoke which is physically located at 919 Lafayette Road, Seabrook, New Hampshire 03874 (**Target Location 3**). WALSH is also listed as the Principal of Adult Video Inc., which does business as Leather & Lace Adult Videos, an adult video and retail store. Leather & Lace is also located at 919 Lafayette Road, Seabrook, New Hampshire 03874, in the space next door to **Target Location 3** (**Target Location 4**).

a. **Target Location 1** is a single-family residence, gray in color with a detached exterior garage, as described in Attachment A. **Target Location 1** is believed to be the location where WALSH lives and operates his businesses, as described in more detail below.

b. **Target Location 2** is a commercial retail suite called The Smoking Monkey

within a business complex described in Attachment A. **Target Location 2** is a business where WALSH distributes synthetic cannabinoids, as described in more detail below.

c. **Target Location 3** is a commercial retail business called Up N Smoke described in Attachment A. **Target Location 3** is a business where WALSH distributes synthetic cannabinoids, as described in more detail below.

d. **Target Location 4** is a commercial retail business called Leather & Lace described in Attachment A. **Target Location 4** is another commercial retail business owned and operated by WALSH that is immediately adjacent to **Target Location 3**. **Target Location 4** is connected to **Target Location 3** by an interior set of double doors, such that customers can move between locations without going outside. WALSH has used accounts associated with the business at **Target Location 4** to pay for synthetic cannabinoids sold at **Target Locations 2 and 3**.

PROBABLE CAUSE

6. In April 2017, state and federal law enforcement in Virginia began a joint investigation into the retail distribution of synthetic cannabinoids from a convenience store at a gas station in Warrenton, Virginia. Synthetic cannabinoids are commonly referred to by the street names "spice", "herbal essence", or "K2." Local law enforcement received intelligence that several individuals had been admitted to local emergency rooms after having consumed quantities of synthetic cannabinoids purchased from the gas station in Warrenton. Through a series of undercover buys, investigators seized several quantities of synthetic cannabinoids containing Schedule I controlled substances from the owners of the gas station.

7. In December 2017, law enforcement executed search warrants in connection with the investigation in Virginia. Pursuant to the search warrant, investigators seized more than seven kilograms of synthetic cannabinoids, as well as approximately $420,611.11 in U.S. currency. A target of the Virginia investigation agreed to cooperate with law enforcement, and will hereinafter be referred to as "CW1." CW1 will be referred to herein in the masculine, regardless of true gender. CW1 admitted that he had purchased synthetic cannabinoids from an online website called "Aroma Superstore," which marketed synthetic cannabinoids as "herbal incense."

8. Investigators identified Joseph Ruis ("RUIS"), Kimberly Drumm ("DRUMM"), and Bonnie Turner ("TURNER") as the primary targets of the investigation and suppliers to the Virginia gas station operators through an analysis of bank records and business records, in conjunction with physical surveillance, toll record analysis, and controlled purchases of synthetic cannabinoids, as set forth in greater detail below. From that investigation, WALSH was identified as another retail distributor of synthetic cannabinoids that he purchased from RUIS, DRUMM, and TURNER through their spice businesses.

9. Starting in early 2018, law enforcement conducted a series of controlled purchases of synthetic cannabinoids from a company identifying itself as "Aroma Superstore." Most of the synthetic cannabinoids that have been seized in this investigation have tested positive for Schedule I controlled substances, including 5-Fluoro-ADB, FUB-AMB, and ADB-FUBINACA. These are all types of synthetic cannabinoids.

10. When CW1 made purchases of synthetic cannabinoids at the direction of law enforcement, the employees of Aroma Superstore directed the cooperating witness to pay by cashier's checks made out to "New World Marketing" or other entities determined to be linked to RUIS, DRUMM, and/or TURNER. Investigators were able to trace the bank accounts into which

the cashier's checks were deposited, and found that the signature card for the account associated with the entity "New World Marketing" bore RUIS's name. Records associated with the "New World Marketing" accounts showed that large amounts of cashier's checks and money orders were deposited into the accounts, apparently to pay for purchases of synthetic cannabinoids. Additionally, dozens of checks were written on the accounts to numerous other entities, which were determined to be held by or associated with RUIS, DRUMM, and/or TURNER.

11. Based on financial records and incorporation documents, law enforcement has linked RUIS to the following entities: Aroma Superstore, New World Marketing Inc., New World Enterprises, New World Holdings Inc., Little Morongo Land DHS LLC, International Cannabis Group, Desert Fulfillment & Logistics Inc., Aroma Cartel, New World Commerce, Consolidated Fulfillment & Logistics LLC, Yes Vapors Inc., Mad Chemist Inc., Nationwide Aroma Inc., and Brooklyn Group Inc.

12. Based on financial records and incorporation documents, law enforcement has linked DRUMM to the following entities: Aroma Superstore, New World Marketing Inc., Eliquid Mixer Inc., Clear Gold Inc., Aromaplex Inc., and New World Enterprises.

13. Based on financial records and incorporation documents, law enforcement has linked TURNER to the following entities: New World Marketing Inc., New World Holdings Inc., NOCACO Inc., Desert Fulfillment & Logistics LLC, and Mountain Rose Trading Inc.

14. Based on financial records, interviews, and search warrant evidence, law enforcement has identified WALSH as a buyer of spice supplied by RUIS, DRUMM, and TURNER which WALSH then distributes through his retail stores the Smoking Monkey (**Target Location 2**) and Up N Smoke (**Target Location 3**). WALSH has used accounts associated with Leather & Lace Adult Videos (**Target Location 4**) to pay for wholesale shipments of spice.

I. Controlled Purchases of Synthetic Cannabinoids From Aroma Superstore

15. CW1 advised that his contact at Aroma Superstore was someone named "Harvey," whom he reached by calling the phone number (702) 208-9770, which was the public number for Aroma Superstore listed on its website. CW1 advised that "Harvey" instructed him to send payment for the synthetic cannabinoids via cashier's check to "New World Marketing" and/or "New World Holdings." Law enforcement subsequently used CW1 to conduct the series of controlled purchases of synthetic cannabinoids from Aroma Superstore set forth in the table below:

Purchase Date	**Product Purchased**	**Substance**	**Payment Remitted**
02/13/18	133 silver envelopes each containing a leafy substance. Envelopes were labeled "Get Real," "Diablo," "24 Monkey," and "Bizarro."	FUB-AMB (Schedule I)	Cashier's check ($1,449.38)
03/26/18	24 clear glass bottles with black tops labeled "Bizarro 10ml," each containing a clear liquid. One vial was labeled "Cloud 9." The box also contained sealed white envelopes. One of the envelopes was labeled "Aroma Horror Story."	FUB-AMB (Schedule I)	Cashier's check ($1,200)
06/06/18	250 silver envelopes, each containing a leafy substance, with a variety of labels including but not limited to "Atomic Kush," "Bizarro," "California Dreams," and "Bomb Marley." Four 5-milliliter plastic bottles, each containing a clear liquid, each bearing a label "Klimax Berry" or "XXX Strawberry Splash."	FUB-AMB, ADB-FUBINACA (Schedule I)	Cashier's check ($1,006.15)
09/24/18	21 silver envelopes, each containing a leafy substance, labeled "Mad Hatter." Four 5-milliliter plastic bottles, each containing a clear liquid, each bearing a label "Get Real Blazing Blueberry," Bubble Yum Orgazmo," and "Strawberry Splash."	FUB-AMB (Schedule I)	Credit card

Purchase Date	Product Purchased	Substance	Payment Remitted
04/03/19	47 silver envelopes, each containing a leafy substance with a variety of labels including but not limited to "Bizarro Hypnotic," "24 K Monkey," and "Make Aroma Great Again."	ADB-FUBINACA (Schedule I)[1]	Cashier's check ($698.14)

II. Identification of Walsh

16. Law enforcement interviewed a former employee of the businesses owned and operated by RUIS, DRUMM, and TURNER. This person will hereinafter be referred to as "CW2" (cooperating witness 2). CW2 will be referred to in the masculine regardless of true gender. CW2 was familiar with the methods by which RUIS, DRUMM, and TURNER operated their businesses and sold synthetic cannabinoids to various customers around the country. CW2 stated that some customers placed wholesale orders, which were orders of a pound or more. CW2 stated that RUIS maintained a list of large-scale buyers of spice that he (RUIS) referred to as "whales." CW2 identified WALSH as a "whale" based in New Hampshire who was RUIS's second largest customer.

17. CW2 stated that WALSH placed orders for between $6,000 and $10,000 worth of spice and typically paid with two separate checks because the orders were for both of WALSH's businesses (Smoking Monkey, and Up In Smoke). CW2 further explained that when WALSH called to place an order from the Aroma Superstore website, WALSH would verbally identify himself by saying, "This is WALSH from Up N Smoke."

[1] Not all lab reports have come back from this controlled purchase, but the ones that have been completed have shown that the tested packets contained ADB-FUBINACA, a Schedule I controlled substance.

III. Financial Links Between RUIS, DRUMM, TURNER, and WALSH

18. A review of bank records associated with accounts linked to RUIS, DRUMM, TURNER, and associated business entities revealed that RUIS, DRUMM, and TURNER appear to be moving the proceeds of their synthetic cannabinoid sales between various accounts at different financial institutions. Analysis of these various accounts showed payments made by WALSH consistent with payments made for the purchase of spice.

The 9943 Account (New World Marketing / Joseph RUIS)

19. During the course of the investigation, agents identified a US Bank account, ending in 9943 (hereinafter, the 9943 Account) held in the name of New World Marketing. The signature card for the 9943 Account was listed under Joseph RUIS, with the phone number (212) 744-3388. Bank records for the 9943 Account reveal that a total of approximately $1,009,169.13 in money orders and cashier's check deposits were made by customers throughout the United States for the time period of approximately January 2017 through December 2018. Deposits were made on a nearly daily basis. The money orders and cashier's checks deposited into the 9943 Account resemble the same method of payment that the Aroma Superstore/New World Marketing employees instructed CW1 to use.

20. Bank records for the 9943 Account also reveal a total of $51,280.96 in deposits sent from WALSH, including the below checks written to New World Marketing and signed by WALSH.

Date	Payee Name	Payee Account	Instrument	Amount	Notes
04/02/18	New World Marketing	Smoking Monkey, Inc.	CHK 2742	$5250.95	Signed by WALSH

04/02/18	New World Marketing	Smoker's City LTD	CHK 3993	$5250.95	Signed by WALSH
04/06/18	New World Marketing	Smoker's City LTD	CHK 4000	$5250.00	Signed by WALSH
04/06/18	New World Marketing	Smoking Monkey, Inc.	CHK 2751	$5250.00	Signed by WALSH
04/18/18	New World Marketing	Smoking Monkey, Inc.	CHK 2763	$2509.53	Signed by WALSH
04/18/18	New World Marketing	Smoker's City LTD	CHK 4013	$2509.53	Signed by WALSH
05/01/18	New World Marketing	Smoker's City LTD	CHK 4019	$3,000.00	Signed by WALSH
05/01/18	New World Marketing	Smoking Monkey, Inc.	CHK 2769	$3,000.00	Signed by WALSH
05/29/18	New World Marketing	Smoker's City LTD	CHK 4041	$3,330.00	Signed by WALSH
05/29/18	New World Marketing	Smoking Monkey, Inc.	CHK 2792	$3,330.00	Signed by WALSH
06/12/18	New World Marketing	Smoker's City LTD	CHK 4052	$3,300.00	Signed by WALSH
06/12/18	New World Marketing	Smoking Monkey, Inc.	CHK 2805	$3,300.00	Signed by WALSH
06/27/18	New World Marketing	Smoking Monkey, Inc.	CHK 2820	$3,000.00	Signed by WALSH
06/27/18	New World Marketing	Smoker's City LTD	CHK 4067	$3,000.00	Signed by WALSH

The 2005 Account (Desert Fulfillment – Logistics LLC / Bonnie TURNER)

21. During the course of the investigation, agents also identified a Wells Fargo account, ending in 2005 (hereinafter, the 2005 Account), held in the name of Desert Fulfillment - Logistics

LLC also known as Desert Fulfillment & Logistics LLC and DFL. Bank records for the 2005 Account revealed that the signature card dated June 26, 2018 lists Bonnie TURNER.

22. Between in and around August 2018 and April 2019, bank records reveal that there was a total of approximately $809,279.60 in deposits into the 2005 Account. Those deposits included money orders and cashier's checks from various people throughout the United States. Those financial instruments that were deposited resemble the same method of payment that the Aroma Superstore/New World Marketing employees instructed CW1 to use.

23. Bank records for the 2005 Account also reveal a total of $129,893.50 USD deposits in funds sent by WALSH including the below checks written to Desert Fulfillment and Logistics and signed by WALSH.

Date	**Payee Name**	**Payee Account**	**Instrument**	**Amount**	**Notes**
08/23/18	Desert Fulfillment Logistics	Smoking Monkey, Inc.	CHK 2867	$3175.90	Signed by WALSH
08/23/18	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4111	$3175.85	Signed by WALSH
09/17/18	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4132	$4224.48	Signed by WALSH
09/17/18	Desert Fulfillment Logistics	Smoking Monkey, Inc.	CHK 2889	$4224.47	Signed by WALSH
10/09/18	Desert Fulfillment Logistics	Smoking Monkey, Inc.	CHK 2906	$4000.00	Signed by WALSH
10/09/18	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4147	$4000.00	Signed by WALSH

12/03/18	Desert Fulfillment Logistics	Smokers City LTD	CHK 4189	$3046.40	Signed by WALSH
12/03/18	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 2952	$3046.40	Signed by WALSH
12/10/18	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4195	$4000.00	Signed by WALSH
12/10/18	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 2960	$4000.00	Signed by WALSH
01/07/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 2981	$3000.00	Signed by WALSH
01/07/19	Desert Fulfillment Logistics	Smokers City LTD	CHK 4210	$3000.00	Signed by WALSH
01/16/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 2986	$3000.00	Signed by WALSH
01/16/19	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4214	$3000.00	Signed by WALSH
01/31/19	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4225	$3000.00	Signed by WALSH
01/31/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 2997	$3000.00	Signed by WALSH
02/07/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3004	$3000.00	Signed by WALSH
02/07/19	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4232	$3000.00	Signed by WALSH

02/13/19	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4238	$3000.00	Signed by WALSH
02/13/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3011	$3000.00	Signed by WALSH
02/22/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3017	$3000.00	Signed by WALSH
02/22/19	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4244	$3000.00	Signed by WALSH
02/26/19	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4251	$3000.00	Signed by WALSH
02/26/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3024	$3000.00	Signed by WALSH
03/06/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3032	$3000.00	Signed by WALSH
03/06/19	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4259	$3000.00	Signed by WALSH
03/14/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3040	$3000.00	Signed by WALSH
03/14/19	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4265	$3000.00	Signed by WALSH
03/20/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3047	$3000.00	Signed by WALSH
03/20/19	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4272	$3000.00	Signed by WALSH

03/29/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3054	$3000.00	Signed by WALSH
03/29/19	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4280	$3000.00	Signed by WALSH
04/01/19	Desert Fulfillment Logistics	Smoker's City LTD	CHK 4285	$4500.00	Signed by WALSH
04/01/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3059	$4500.00	Signed by WALSH
04/09/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3067	$3000.00	Signed by WALSH
04/14/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3074	$6000.00	Signed by WALSH
04/15/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3073	$3000.00	Signed by WALSH
04/22/19	Desert Fulfillment Logistics	Smoking Monkey Inc.	CHK 3080	$6000.00	Signed by WALSH

Additional Check Signed by WALSH Mailed to New World Marketing

24. On July 18, 2019, United States Postal Inspection Service was issued a search and seizure warrant for 35 items of United States Postal Service Mail in association with a commercial mail receiving agency ("CMRA") box held by or for Joseph RUIS. CW1 was instructed to remit payment to this CMRA box for the June 2018 and April 2019 controlled purchases of spice from the Aroma Superstore website described in above. One of the seized mail parcels was from AVI with a return address of "919 Lafayette Rd, Seabrook, N.H. 03874," which corresponds to **Target**

Locations 3 and 4, and was addressed to New World Marketing at "36101 Bob Hope Drive, Suite E-5 Box 220, Rancho Mirage, CA. 92270."[2] AVI, or "Adult Video Inc.," is doing business as Leather & Lace Adult Videos, which is located at **Target Location 4**. As noted above, WALSH also owns and operates, and is listed on business filings for, Leather & Lace.

25. Inside this mail parcel was a business check from S.M.I. (Smoking Monkey Inc.), made payable to DFL,[3] in the amount of $6,000.00 USD signed by WALSH and dated May 21, 2019. In a review of financial records, the check was written on a Provident Bank account (ending in 9330) associated with Smoking Monkey Inc.

IV. Controlled Purchases of Synthetic Cannabinoids From WALSH

26. Beginning in and around June 2017, the Seabrook, New Hampshire, Police Department ("SPD") conducted a series of controlled and/or undercover purchases of synthetic cannabinoids using either a confidential informant ("CI") or undercover officer ("UC"). In each transaction, the packages seized resembled the packages purchased directly from Aroma Superstore by law enforcement in Virginia. The controlled purchases from WALSH are summarized in the table below:

Date	**Buyer**	**Purchase Price**	**Quantity**	**Substance**	**Location**
06/29/17	CI	$40	Two 1.5-gm packages labeled "Mad Hatter" and "Aces High Strawberry	FUB-AMB ("Mad Hatter"); 5F-AB-PINACA ("Aces High Strawberry")[4]	**Target Location 2**
09/24/18	UC	$60	One 10-gm	ADB-	**Target**

[2] The sender and recipient information on this parcel is listed as it appears on the parcel, including with respect to capitalization, punctuation, and the spelling of addresses.
[3] DFL is believed to be short for Desert Fulfillment Logistics, a company associated with RUIS, DRUMM, and TURNER.
[4] While these substances were not listed on the federal schedule at the time of purchase, both substances had chemical structure similarities to Schedule I controlled substances AB-PINACA and MDMB-FUBINACA. FUB-AMB is now listed as Schedule I controlled substances.

			package labeled "Mad Hatter"	FUBINACA	**Location 2**
09/24/18	UC	$60	One 10-gm package labeled "Mad Hatter"	ADB-FUBINACA	**Target Location 3**
10/03/19	UC	$70	One 10-gm package labeled "Cloud 9 Second Generation Mad Hatter Incense."	Lab results have not yet come back.	**Target Location 2**
10/03/19	UC	$70	One 10-gm package labeled "Cloud 9 Second Generation Mad Hatter Incense."	Lab results have not yet come back.	**Target Location 3**

VI. Overdoses Connected to WALSH's Sales of Spice

27. On September 6, 2018, SPD received information from the New Hampshire Medical Examiner's Office concerning a fatal overdose suspected to be caused by synthetic cannabinoids. The medical examiner provided the contact information for a friend of the deceased, who will hereinafter be referred to as "CW3." CW3 will be referred to herein in the masculine, regardless of true gender. CW3 stated that the deceased smoked Mad Hatter Blueberry spice, which CW3 believed was purchased from **Target Location 2** (The Smoking Monkey) for $60.00 in July 2018. Historically, CW3 stated he purchased spice for himself from **Target Location 2**; however, CW3 suffered from his own overdose which left him hospitalized in a coma for multiple days in July 2018. CW3 provided SPD with the packaging and remaining Mad Hatter Blueberry spice that the deceased smoked prior to his overdose. A chemical analysis of the synthetic cannabinoid turned over to law enforcement confirmed the presence of ADB-FUBINACA, a Schedule I synthetic cannabinoid. The official cause of death of the decedent was listed as complications of rhabdomyolysis due to acute intoxication by ADB-FUBINACA.

28. On May 20, 2019, SPD received a call from an individual who stated that her son purchased spice from Target Location 2 and Target Location 3. This individual was distraught because her son had overdosed on synthetic cannabinoids and was hospitalized. The individual stated that she recovered a small baggie containing spice from her son's car, and that her husband's credit card was missing but there was a $15 charge on it from **Target Location 2**.

VII. Activities at WALSH's Residence (Target Location 1)

29. On April 3, 2019, SPD responded to **Target Location 1** for a reported suicide. As it turned out, WALSH's wife had committed suicide. WALSH was present at **Target Location 1** when officers arrived and allowed them to enter the home. Photographs taken by officers on this day captured images of mail from Bank Card USA, a merchant service for The Smoking Monkey Inc. The mailings from Bank Card USA were addressed to 6 Smiths Lane, Unit 7, Seabrook, New Hampshire, 03874, which is the previous address for The Smoking Monkey retail store. The photographs from **Target Location 1** also show a mailing from the Department of the Treasury, Internal Revenue Service, addressed to Smoking Monkey Inc. at an address in Seabrook associated with WALSH. Finally, a mailing from a CPA addressed to Smoking Monkey, Inc, Attn. Bill WALSH was found at **Target Location 1**. The presence of these mailings at **Target Location 1** demonstrates WALSH utilizes his home residence for business purposes and maintains documents associated with the business through which he is selling synthetic cannabinoids at his residence.

EVIDENCE AT THE PREMISES TO BE SEARCHED

30. Given the evidence and circumstances discussed in this affidavit, there is reason to believe that evidence related to a conspiracy to distribute controlled substances, in violation of 21 U.S.C. §§ 841(a)(1) and 846, will be found within the **Target Locations**. Specifically, there is probable cause to believe that WALSH, who exercises control over the **Target Locations**, is

actively involved in the foregoing offenses and maintains within the **Target Locations** items related to such conduct.

31. This conclusion is further supported by my experience, training, and knowledge of this investigation as related to the distribution of controlled substances, through which I am aware of the following information:

a. Drug traffickers commonly maintain at their residences and on their property additional quantities of the illicit drugs being distributed, as well as packaging materials, scales, owe sheets, and other drug paraphernalia in their residences or on their property. Such contraband may be concealed in locations known to the traffickers to avoid law enforcement detection.

b. Drug traffickers commonly maintain at their residences and on their property books, records, receipts, mobile data storage units, computers, notes, ledgers, airline tickets, money orders, passports, visas, and other papers relating to the transportation, purchase, packaging, sale, and distribution of controlled substances.

c. Drug traffickers commonly maintain in their residences and on their property books, paper, and other records which reflect the names, addresses, and telephone numbers of their suppliers, couriers, customers, and other associates in the illegal drug trade.

d. Drug traffickers commonly maintain books, papers, and documents in secure locations within their residences and their property, so they can have ready access to such information, including documents related to their rental or occupancy of their residence and financial records. These financial records include receipts, wire transfers,

money orders that aid in the concealment and transfer of proceeds from their illicit drug trade.

e. Drug traffickers attempt to legitimize the proceeds from the sale of controlled substances. Books and papers relating to such efforts, including cashier checks, money orders, and ledgers are maintained in the residences and on the property of the drug trafficker. Drug traffickers often keep information and/or currency relating to their illicit drug trade in locked or closed containers in their residence in an attempt to secure these items.

f. Drug traffickers take, or cause to be taken, photographs and/or videos of themselves, their associates in the drug trade, property derived from the distribution of narcotics, and their products, and that such photographs and/or videos are often kept in their residences.

g. Drug traffickers commonly make attempts to conceal contraband in vehicles for the purpose of transportation.

h. Drug traffickers very often place assets, including real and personal property, such as vehicles, in names other than their own to avoid the detection and forfeiture of such assets by government agencies and continue to use these assets and to exercise dominion and control over them even though the assets are normally owned by them.

32. Furthermore, based on my experience, training, and knowledge of this investigation as it relates to money laundering and/or structured financial transactions, I am aware of the following information:

a. It is common for individuals involved in financial crimes to hide the proceeds and records of such financial crimes — including but not limited to books, records, receipts, notes, ledgers, business and personal checks, business and individual checking account and brokerage account statements, credit cards, credit card statements, account numbers, access numbers, and false identifications — within their residences and offices/businesses, for ready access and also to conceal such items from law enforcement. These individuals will often deposit monies derived from an illegal activity into bank or brokerage accounts that they maintain, and then use those monies through wire transfers and other withdrawals and checks written from the accounts.

b. Individuals engaging in financial crimes such as money laundering and structuring transactions will commonly convert the proceeds from unlawful activities into other assets such as real property, investments, automobiles, boats, and aircraft. I also know that it is a common practice of individuals involved in money laundering to maintain at their residences, places of business, and other sites to which they have access, records such as (1) corporate and accounting records, (2) telephone bills and statements, (3) banking, brokerage, and investment files and records, and (4) correspondence with co-conspirators which are related to their illegal activities.

c. Individuals engaged in financial crimes often conceal large amounts of currency, financial instruments, precious metals, jewelry and other things of value and/or proceeds of financial transactions made from engaging in financial crimes within their residences, offices/businesses, garages, storage buildings, automobiles, and safety deposit boxes.

d. Money service businesses, whether licensed or not, necessarily require the production and retention of records on the business premises and/or in the personal residences indicative of the acquisition and disposition of large sums of currency and/or currency equivalents. The records produced and retained include the types of records identified in Attachment B, which is incorporated herein.

33. I also know through my training, experience, and knowledge of this investigation, that it is common to maintain and store the aforementioned evidence, in particular of financial crimes, electronically, using computer hardware, software, electronic storage devices, and different types of computer media, as discussed more fully below.

ELECTRONIC EVIDENCE

34. Pursuant to Rule 41(e)(2)(B), the warrant applied for would also authorize the seizure, or, potentially, the copying, of electronically stored information within any seized digital devices and electronic storage media. As used herein, the terms "electronic storage media" and digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

35. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that if electronic storage media or digital devices are found in the subject premises, there is probable cause to believe that the records and information described in Attachment B will be stored in such media or devices for, but not limited to, the following reasons:

a. Individuals who engage in criminal activities, in particular financial crimes, use digital devices to communicate with co-conspirators online, but they also store on computer hard drives and other electronic storage media records relating to their illegal activity. Online criminals store these documents and records, which can include logs of online "chats" with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social media accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things:

i. keep track of co-conspirators' contact information;

ii. keep a record of illegal transactions for future reference;

iii. keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and

iv. store stolen data for future exploitation.

b. Individuals engaging in the criminal activities, in the event that they change computers, will often "back up" or transfer files from their old computers' hard drives to

that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Computer, smart phone, and other digital device files, or remnants of such files, can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space — that is, in space on the storage medium that is not currently being used by an active file — for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

e. Wholly apart from user-generated files, computer storage media — in particular, computers' internal hard drives — contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

f. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from an electronic storage medium depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

36. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the seized items were used, the purpose of their use, who used them, and when. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the Target Locations because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other

external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

e. I know that when an individual uses a digital device to engage in criminal activities, including criminal conspiracies, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital

device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

37. *Methods to be used to search digital devices.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals, specialized equipment, and software programs necessary to conduct a thorough search. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery

of "residue" of electronic files from electronic storage media also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises. Smart phones capable of storing 64 gigabytes, flash drives capable of storing 128 gigabytes, and desktop computers capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain enormous amounts of data.

d. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not able to be segregated from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

e. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that

the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

f. Analyzing the contents of mobile devices can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable

and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

g. Based on all of the foregoing, I respectfully submit that searching any electronic storage media or digital device for the information, records, or evidence subject to seizure pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the media or devices. In light of these difficulties, I request permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

38. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

39. Based on the information discussed above, the specific items to be seized are described and detailed in Attachment B.

CONCLUSION

40. Based on the information provided in this affidavit, I submit that there is probable cause to believe that the items set forth in Attachment B will be found within the **Target Locations** described in Attachment A and that such items constitute evidence related to the distribution of controlled substances, and any attempts and/or conspiracies to do the same, in violation of Title 21, United States Code, Sections 841(a)(1) and 846.

41. Wherefore, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, I respectfully request warrants to search **Target Locations 1**, **Target Location 2**, and **Target Location 3**, which are all located within the District of New Hampshire.

42. I declare under penalty of perjury that the statements above are true and correct to the best of my knowledge and belief.

_____
Derek Dunn
Special Agent
Homeland Security Investigations

Sworn and subscribed to me on _____, 2019.

_____
The Honorable
United States Magistrate Judge